**Virtual Private Network VPN**

**Definition**

A VPN can be further defined as follows:

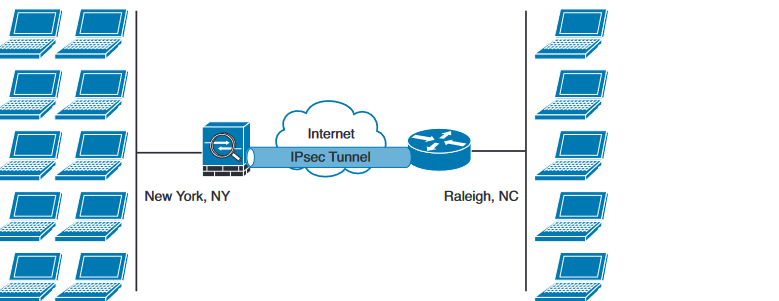
* **Virtual:** Logical networks, independent of physical architecture
* **Private:** Provides privacy using two approaches:
  1. Noncryptographic approach: Independent of IP addressing and routing schemes
  2. Cryptographic approaches: Provides confidentiality, integrity, and authentication
* **Network**: Interconnected computers, devices, and resources grouped to share information
* Organizations deploy VPNs to provide data integrity, authentication, and data encryption to ensure confidentiality of the packets sent over an unprotected network or the internet
* VPNs protect data that is transmitted over a public or shared infrastructure such as the Internet from threats such as man-in-the-middle attacks.

**VPN Benefits**

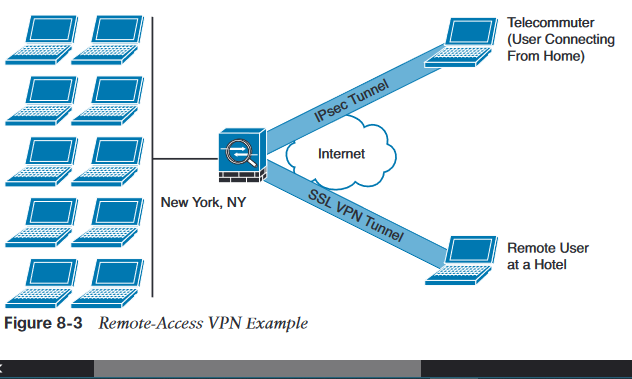
* Eliminate expensive dedicated wan links
* Scalability: enable corporations to use the internet infrastructure within ISPs and devices, which makes it easy to add new users.
* High speed broadband connectivity
* Security: VPNs provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.

**Virtual Private Network VPN implementations groups**

* **Site-to-site VPNs:** enable organizations to establish VPN tunnels between two or more network infrastructure devices in different sites



* **Remote-access VPNs:** enable users to work from remote locations such as their homes, hotels, and other premises as if they were directly connected to their corporate network



**VPN components**

* **Authentication:** to verify the identity of a device or user before allowing it to establish a VPN connection to your network.
* **Encapsulation Method:** how user information, such as data, is to be encapsulated and transported across a network. Encapsulation also defines which applications or protocols can be placed in the payload of a VPN packet
* **Data Encryption:** Data encryption basically takes user data and a key value and runs it through an encryption algorithm, producing what looks like a random string of characters. Only a device with the same key value can decrypt the information. Encryption algorithms (DES, 3DES, AES, Blowfish, RSA, IDEA, RC4…).
* **Packet Integrity**
* **Key management**
* **Non**-**repudiation:** In the VPN world, non-repudiation involves two components: authentication and accounting. Authentication verifies the identity of a device or user before allowing it to establish a VPN connection to your network. Accounting is the recording of the VPN session
* **Application and Protocol Support:** When choosing a VPN implementation, you'll need to first determine which types of traffic need to be protected. For example, if you only have IP traffic in your network, most VPN implementations will be available to you.
* **Address Management:**

**Protocols that have been used throughout the years for VPN implementations:**

* + PPTP Point to point Tunneling Protocol
  + L2F Layer 2 Forwarding Protocol
  + L2TP Layer 2 Tunneling Protocol
  + GRE Generic Routing Encapsulation Protocol
  + MPLS VPN: Multiprotocol Label Switching
  + IPsec Internet Protocol Security
  + SSL
* L2F, L2TP, GRE and MPLS VPNs do not provide data integrity, authentication, and data encryption; you can combine these protocols with IPsec to provide these benefits

**Secure VPN Implementations protocols**

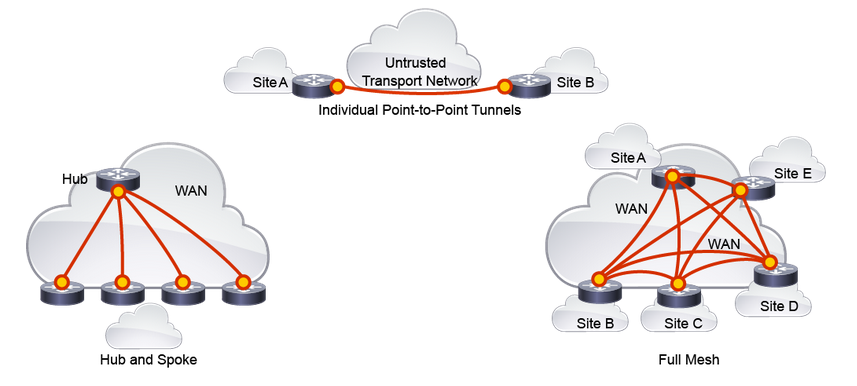
* IP security (IPsec) for remote access and site-to-site
* Secure Socket Layer (SSL) / Transport Layer Security (TLS) for remote access, allows to access a network using a browser

**Insecure VPN Implementations protocols**

* Generic Routing Encapsulation (GRE)
* DMVPN, L2F, L2TP, GRE and MPLS VPNs

**Site to Site VPN Topologies**

Three typical logical VPN topologies are used in site-to-site VPNs: **Individual point-to-point VPN connection, Hub and spoke, full mesh**



In addition to the three main VPN topologies, these additional complex topologies can be created:

* **Partial mesh:**
* **Tiered hub-and-spoke:** A network of hub-and-spoke topologies in which a device can behave as a hub in one or more topologies and a spoke in other topologies.
* **Joined hub-and-spoke:** A combination of two topologies (hub-and-spoke, point-to-point, or full mesh) that connect to form a point-to-point tunnel.

**Site to Site High Availability Overview**

Possible failures in a VPN deployment are: Transport network failure, VPN device failure, VPN device link/interface failure

Solutions: Redundant transport network, redundant VPN device, redundant interface on the VPN device

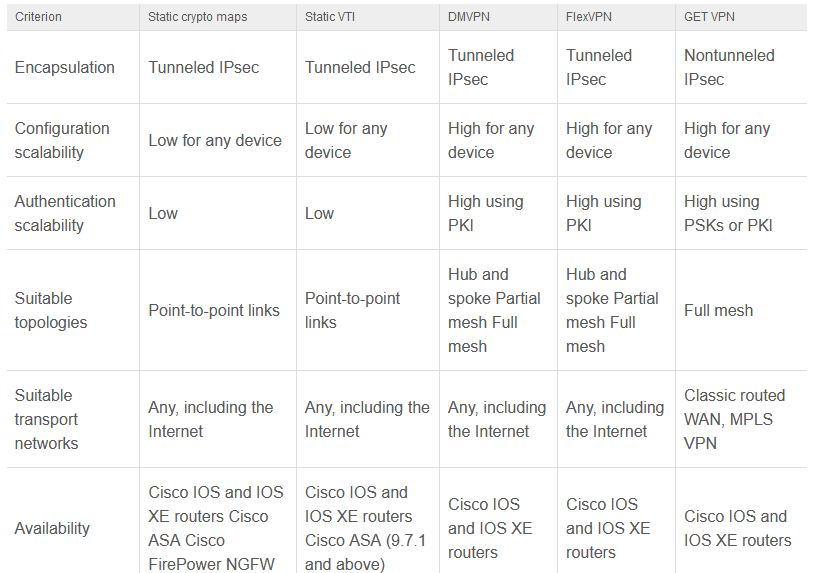
**Site-to-Site VPN Technologies**

Site-to-Site VPNs have the following properties:

* Connect sites as a replacement for a classic WAN
* Work over controlled networks (MPLS) or Internet transport networks
* Often require high availability and performance guarantees (QoS)
* Can be configured in several different ways and on different devices

**VPN technologies and implementations that are available on Cisco devices:**

* Static crypto maps
* Static virtual tunnel interface
* Cisco DMVPN
* Cisco GET VPN
* Cisco FlexVPN



**IPsec VPN**

* Defined in RFC 4301
* Combines three protocols into a cohesive security framework:
* **1 Encapsulation Security Payload (ESP):** provides an encapsulation for encryption and authentication of user traffic
* **2 Authentication Header (AH):** provides an encapsulation for authentication of user traffic (obsolete)
* **3 IKE/IKEv2**: provides a framework for policy negotiation and key management

IPsec uses two modes to encapsulate the data:

* **IPsec transport mode:** the original IP header is preserved and no other IP header is added; so routing is done based on the true destination and/or source IP address.
* **IPsec tunnel mode**: the original IP header (inner header) is preserved and a new outer IP outer header is used, identifying the tunnel endpoints; so routing is done based on the new outer header, which is the destination and source of the IPsec tunnel.

**Internet Key Exchange**

**IKEv1**

* Documented in RFC 2408
* Uses phases approach to establish SAs (security association)
* Runs over UDP to destination port 500
* PFS provides additional security if needed

**IKEv1 Phase1 (create an IKE SA)**

In this phase several attributes are exchanged: encryption algorithms, hashing algorithms, Diffie-Hellman groups, authentication method, vendor-specific attributes

* Traditional encryption algorithms used in IKE: DES (64bits long), 3DES (168 bits long), AES (128 bits long), AES 192, AES 256
* Hashing algorithms: SHA, MD5
* Authentication methods: pre-shared keys (small and medium-size organizations use pre-shared keys), digital certificates with use of PKI (large organizations used this for scalability, centralized management.)

**Two modes to establish a Phase 1 security association (SA):**

* **Main mode:** IPsec peers complete a six-packets exchange in three round trips to negotiate the ISAKMP SA
* **Aggressive mode** completes the SA negotiation in three packet exchanges.

**IKEv1 Phase 2 (creates IPsec SAs)**

* Is used to negotiate the IPsec SAs.

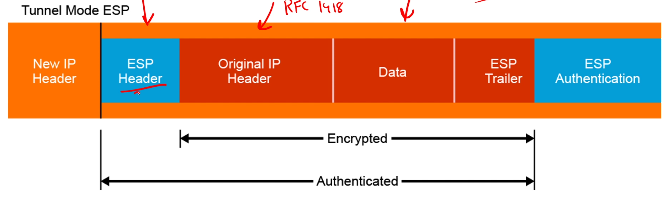
**IKEv2**

* Defined in RFC 4306
* Runs over UDP to destination port 500
* Provides a simpler and more efficient exchange
* Creates the child SAs within the same negotiation, instead of using a phased approach

**Differences between IKEv1 and IKEv2**

* IKEv1 has two possible exchanges (main and aggressive mode); IKEv2 is a single exchange of message pair for IKEv2 IKE\_SA
* IKEv2 has a simple exchange of two message pairs for the CHILD\_SA; IKEv1 uses an exchange of at least three message pairs for Phase 2;
* Fewer packets are exchanged and less bandwidth is needed compared to IKEv1
* IKEv2 supports the use of next-generation encryption protocols and anti-dos capabilities, EAP

**Encapsulating Security Payload**



**NAT Traversal (NAT-T)**

* Allow the VPN peers to dynamically discover whether an address translation device exists between them
* If they detect a NAT/PAT device, they use UDP Port 4500 to encapsulate the data packets

**IPsec Static Crypto Maps**

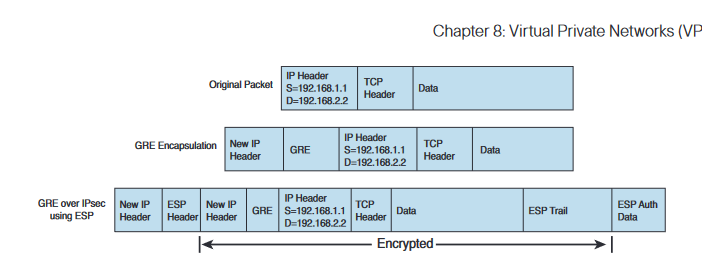
* only a subset of traffic on an interface is encrypted and encapsulated, based on configured policy.
* you create a crypto map object. Within that object you specify the IP address of the VPN peer, the set of cryptographic algorithms that will protect traffic, and access control list (ACL) that defines a subset of traffic that needs to be encrypted. Crypto map is then applied to an interface.

**Tunnel Interfaces**

* An alternative to crypto maps
* This is accomplished by creating a logical interface that represents the source and destination endpoints of the tunnel

**Gre over IPsec**

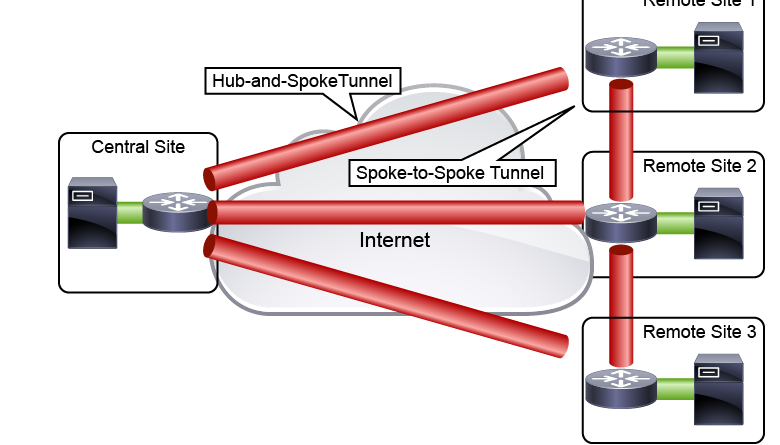
* GRE Provides a simple mechanism to encapsulate packets of any protocol over any other protocol between two endpoints



**IPsec Static Virtual Tunnel Interface**

* replace static crypto map-based configuration
* simplified interface feature support…

**Cisco DMVPN**

* DMVPN (Dynamic Multipoint VPN) is a routing technique we can use to build a VPN network with multiple sites without having to statically configure all devices.
* It’s a “hub and spoke” network where the spokes will be able to communicate with each other directly without having to go through the hub. Encryption is supported through IPsec which makes DMVPN a popular choice for connecting different sites using regular Internet connections

DMVPNs use the following mechanisms to combine the best of hub-and-spoke and fully meshed topologies, as well as provide some other features:

* **Multipoint GRE (mGRE):** mGRE technology enables a single GRE interface to support multiple GRE tunnels and simplifies the complexity of the configuration
* **Next-Hop Resolution Protocol (NHRP):** NHRP is a client and server protocol in which the hub acts as an NHRP server and the spokes act as NHRP clients.
* **IPsec:** IPsec provides transmission protection for GRE tunnels.

**FlexVPN**

* FlexVPN is Cisco’s solution to simplify VPN deployments and covers all VPN types: Site-to-site, Hub and spoke (including spoke-to-spoke traffic), Remote access
* FlexVPN **uses IKEv2 for all VPN types**. IKEv2 is the successor of [IKEv1](https://networklessons.com/cisco/ccie-enterprise-infrastructure/ipsec-internet-protocol-security) and has some interesting features

**Cisco IOS VTIs**

* simplifies the configuration process and provides a simpler alternative to using generic routing encapsulation (GRE) and crypto maps with IPsec
* Two types of VTI interfaces available on Cisco IOS and IOS XE routers: **static VTIs (SVTIs) and dynamic VTIs (DVTIs).**

SVTI

Static VTIs are used for site-to-site connectivity and provide these benefits:

* Always-on connectivity
* IPsec traffic protection
* Routable interface to implement routing and other interface features
* Routing can be implemented either statically or using a dynamic routing protocol

DVTI

Dynamic VTI tunnels are used for hub-and-spoke topologies: